Kotiverkon tietoturva

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulututkinnon opinnäytetyö

Tietotekniikan ko.

Riihimäki, 27.04.2011

Jussi Linnoinen

HAMK
HÄMEEN AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

Tietotekniikan koulutusohjelma
Riihimäki

Työn nimi	Kotiverkon tietoturva
Tekijä	Jussi Linnoinen
Ohjaava opettaja	Raimo Hälinen
Hyväksytty	27.04.2011
Hyväksyjä	

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Riihimäki
Tietotekniikan ko.
Tietoliikenteen suuntautumisvaihtoehto

Tekijä Jussi Linnoinen **Vuosi** 2011

Työn nimi Kotiverkon tietoturva

TIIVISTELMÄ

Opinnäytetyössä tutustuttiin tietoturvaratkaisuihin kotikäyttäjän kannalta.

Opinnäytetyön teoria-osioihin tutustuttiin lukemalla tietoturvaan liittyviä materiaaleja. Työ aloitettiin asentamalla kaikki tarvittavat tietoturva-ohjelmat tietokoneelle. Työtä varten hankittiin myös erillinen langaton tukiasema ja tukiaseman tietoturvaominaisuuksia tarkasteltiin työssä. Testausympäristö koostui tietokoneesta, langattomasta tukiasemasta ja tietokoneelle asennetuista ohjelmista.

Tietokoneelle asennetut tietoturva ohjelmat osoittautuivat riittäviksi kotikäyttäjän kannalta. Avast Antivirus torjui virukset tietokoneella ja Internetissä. Windows seiskan palomuuri toimi riittävän tehokkaasti langattoman tukiaseman palomuurin kanssa. Palomuurien testaus suoritettiin Shield Up-sivuston testeillä ja palomuurit osoittautuivat tarpeeksi tehokkaiksi torjumaan ulkopuolisia hyökkäyksiä vastaan. Tulevaisuudessa kotikäyttäjien pitänee panostaa tietoturvaan enemmän, koska hyökkäykset lisääntyvät myös kotikäyttäjiä vastaan.

Avainsanat Avast Antivirus, Palomuuri, Tietoturva

Sivut 31s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

Riihimäki
Degree Programme in Information Technology
Information Technology

Author Jussi Linnoinen **Year** 2011

Subject of Bachelor's thesis Home network security

ABSTRACT

The purpose of this thesis was to explore security solutions from at home user´s point of view. The theory was familiarized by reading security solution related materials. The research began by installing all the appropriate security software on a home computer. A separate wireless access point was also configured for the research and different security solution characteristics for this access point were also examined.

The test environment consisted of a computer, a wireless access point and the security software programs installed on the computer. The security solutions installed on the computer proved to be adequate from the home user´s point of view.

Avast Antivirus blocked viruses on the computer and Internet. The Windows seven firewall operated effectively enough with the wireless access point. The testing of the firewall was performed with Shields Up – the site´s tests and the firewall turned out to be effective enough to fight against external attacks.

In the future, home user´s should probably invest more in information security because of the increasing attacks directed towards them.

Keywords Avast Antivirus, Firewall, Security

Pages 31p.

TERMIT JA LYHENTEET

Autosandbox – testiympäristö – testiympäristössä voidaan ajaa tiedostoja eristettynä muusta järjestelmästä

DMZ – alue – Demilitarize zone – aliverkko- tarkoittaa fyysista tai loogista aliverkkoa joka yhdistää tietokoneen turvattomampaan alueeseen esim. Internet

IPsec – IP Security Architecture – protokolla yhteyksien suojaamiseen – sen avulla voidaan turvata salauksen todennus ja tietojen eheys.

Ipv6 – IP-protokolla – staattinen IP-protokolla joka tarjoaa suuremman osoiteavaruuden kuin edeltäjänsä ja sitä on yksinkertaistettu pakettien välittämisessä

Mac filtteröinti –Media Access Control filtteröinti - liikenteen suodatus – tarkoitus on suodattaa epätoivotut verkkokortit tukiaseman verkosta

Portforwarding – palveluidenohjaus- sen avulla erilaiset palvelut voidaan ohjata oikeaan porttiin, muuten portti voi olla suljettu

SSID – Service set indentifier – langattoman verkon verkkotunnus – käytetään langattoman verkon mainostukseen lähiverkon tietokoneille

Smurf attack – palvelunestohyökkäys – perustuu tietokoneen hukuttamiseen datapaketeilla

TCP – Transmission Control Protocol – protokolla – jonka avulla voidaan luoda yhteyksiä tietokoneiden välille.

TKIP – Temporal Key Integrity Protocol – tietoturvaprotokolla – se huolehtii tietojen salaamisesta WPA:ssa

UDP – User Datagram Protocol – yhteydetön protokolla – se mahdollistaa tiedon siirron joka ei vaadi yhteyttä laitteiden välille

UPnP – Universal Plug and Play – avulla saadaan erilaiset laitteet kommunikoimaan toistensa kanssa

WEP – Wired Equivalent Privacy – salausmenetelmä – IEEE :n 802.11 standardin ensimmäinen salausmenetelmä langattomalle verkolle

Wlan kortti – Wireless Local Area Network – langattoman lähiverkkotekniikan kortti jolla voidaan muodostaa yhteys langattomaan tukiasemaan

WPA – Wi-Fi Protected Access – tietoturvatekniikka - kehitettiin WEP -salauksen pohjalta, salauksessa vaihdellaan salausavainta tietyin väliajoin

WPA- PSK – Pre-shared key – jaettuavain – langaton tukiasema jakaa avaimet tietokoneiden ottaessa yhteyden langattomaan verkkoon

WPA2 – Wi-Fi Protected Access – tietoturvatekniikka – on kehitetty WPA salauksen pohjalta. WPA 2 tarjoaa paremmat algoritmit, joten sen murtaminen on lähes mahdotonta nykyisillä laitteilla

PORTTILISTA

21/TCP – File Transfer Protocol - FTP

22/TCP, UDP – Secure Shell - SSH

24 Mail, sähköposti

25/SMTP, – Simple Mail Transfer Protocol

79/TCP, – User information Protocol

80/TCP, – Word Wide Web HTTP

110/TCP, - Post Office Protocol – POP 3

113/TCP, – IDENT - palvelu

119/TCP, – USENET - uutisryhmät

135/TCP, – MS Windows etäyhteys

139/TCP, – Netbios – yhteyden hallinta

SISÄLLYS

1 JOHDANTO

Tietoturvallisuudesta on tullut yhä tärkeämpi asia yrityksille ja kuluttajille. Tietokoneessa on hyvä olla palomuuri- ja virusturvaohjelmisto. Internet tarjoaa monia tietoturvaratkaisuja ilmaiseksi.

Tämän opinnäytetyön aiheena on Kotiverkon tietoturva. Opinnäytetyössä käydään läpi tärkeitä aiheita liittyen palomuuriin ja virusturvaan. Lisäksi perehdytään palomuurin ja virusturvan asennukseen ja käyttöönottoon. Opinnäytetyössä käydään läpi Netwjork-reitittimen tietoturvaratkaisuja palomuurin ja langattoman verkon kannalta. Opinnäyte käsittelee palomuurin tärkeimpiä ominaisuuksia ja sääntöjen luomista eri ohjelmille. Työssä käydään läpi virusturvan tärkeimmät ominaisuudet ja viruksen poisto turvallisesti.

Opinnäytetyön laatiminen aloitettiin tutustumalla kyseisiin ohjelmiin.

2 VIRUSTURVA

2.1 Virusturvasta yleisesti

Virustorjunta on tietokoneohjelma, jolla voidaan etsiä ja poistaa viruksia. Virustorjuntaa voidaan suorittaa paikallisesti ja etähallinnalla. Virustorjunnalla on muitakin tärkeitä tehtäviä mm. estää viruksen leviäminen muille tietokoneille verkossa. Virustorjuntaohjelmilla on kaksi tilaa, tiedostojen tarkastus tiettynä aikana ja reaaliaikainen tarkastus. Virustorjunta voidaan määrittää tarkastamaan tiedostot haluttuna ajankohtana.

Reaaliaikainen tila estää tiedostojen saastumisen, koska virustorjunta tarkastaa tiedoston ennen kuin käyttäjä avaa kyseisen tiedoston. Virustorjuntaohjelmistossa virus voidaan laittaa karanteeniin tai aloittaa kyseisen tiedoston puhdistus. Nykyaikaisilla virustorjuntaohjelmistoilla on myös monia erilaisia torjuntamuotoja viruksia vastaan, mm. selainsuoja, verkkosuoja ja pikaviestinsuoja. Selainsuoja valvoo kaikkea selaimen ja verkon välistä liikennettä. Selainsuoja estää virustartunnan leviämisen ennen kuin se ehtii selainohjelmaan. Pikaviestinsuoja suojaa tietokoneen pikaviestiohjelmien kautta leviäviä viruksia vastaan. Virusturvasta on siis tullut osa verkkopalveluita. Joka viikko tulee uusia haittaohjelmia, joten sen takia on tärkeä pitää virustorjuntaohjelmisto ajan tasalla uusimpia tartuntoja vastaan. Suurin osa tartunnoista saadaan sähköpostin välityksellä.
(Fidora, 2011.)

2.2 Heikkoudet

Virustorjunnan tärkein tarkoitus on se, että ohjelmisto tekee reaalitarkastuksia uusille tiedostoille ennen käyttäjän toimia ja koko tietokoneen tarkastukset säännöllisesti. Virustorjunta ei kuitenkaan aina välttämättä suojaa kaikkia viruksia vastaan, koska uusia viruksia tulee viikoittain. Virustorjunta ohjelmisto saattaa joskus mennä sekaisin ja silloin tietokoneen saattaa joutua käynnistämään uudelleen. Virustorjunta pitää päivittää tasaisin väliajoin, jotta se tunnistaisi uusimmat virukset ja haittaohjelmat.
(Fidora, 2011.)

2.3 Avast Antivirus

Avast on tšekkiläinen Avast Softwaren tekemä virustorjuntaohjelma Windows ja Linux-käyttöjärjestelmille. Ensimmäinen versio Avastista julkaistiin vuonna 1988 ja ohjelman kotiversio on todella suosittu Windows käyttöjärjestelmän käyttäjien keskuudessa. Avast Antivirusta on saatavilla 27 eri kielellä. Avastin voi asentaa palvelimelle ja normaaliin kotikäyttöön. (Wikipedia, 2011.)

2.4 Tärkeimpiä ominaisuuksia

Alla olevasta listasta selviää Avast Antiviruksen tärkeimmät ominaisuudet. Avast tarjoaa monia hienoja ominaisuuksia, joita ei välttämättä ole maksullisissa versioissa.

- File System Shield
  reaaliaikainen suojaus eli se tarkastaa tiedostoja koko ajan
- Mail Shield
  suojaa sähköpostiin tulevilta viruksilta
- Web shield
  suojaa selaimen kautta tulevia viruksia muun muassa tarkistamalla www-selaimen linkkejä
- P2P shield
  suojaa viruksia vertaisverkossa
- IM Shield
  suojaa mahdollisilta viruksilta esimerkiksi Msn Messengerissä
- Network shield
  Suojaa tunnettuja matoja vastaan, esimerkiksi Blasteria vastaan
- Behavior Shield
  ilmoittaa järjestelmän toiminnasta jos siinä on jotakin epäilyttävää
- Audible alarms
  Äänivaroitukset käyttäjälle
- Automaattiset päivitykset
  Automaattiset päivitykset huolehtivat että virustorjunnan tietokannat pysyvät ajan tasalla ilman käyttäjän toimenpiteitä.

(Wikipedia, 2011.)

2.5 Järjestelmän vaatimukset

Avast Antivirus järjestelmän vaatimukset ovat pienet. Järjestelmävaatimuksissa pitää ottaa huomioon, että vaatimukset ovat suuntaa antavia ja tietokone ei välttämättä toimi kyseisellä ohjelmalla hyvin vähimmäisvaatimuksilla. Taulukosta 1 selviää vähimmäisvaatimukset Avast Antivirukselle.

Taulukko 1 Tietokoneen vähimmäisvaatimukset

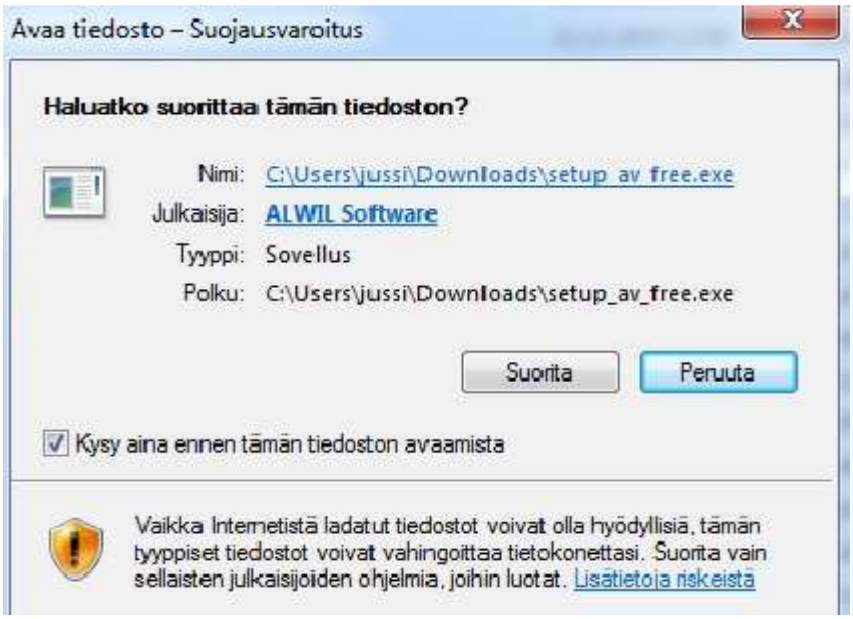
tietokoneen suoritin	keskusmuisti	kovalevytila	käyttöjärjestelmä
Intel Pentium 3 tai vastaava	128 MB RAM	100 MB	Microsoft Windows 2000, XP, Vista ,7 (32/64 bit)

3 VIRUSTURVAN ASENNUS JA KÄYTTÖ

Virusturvan asennus aloitettiin lataamalla Avast Antivirus Avastin Internet-sivuilta. Tämän jälkeen aloitettiin ohjelman asennus.

3.1 Avast Antiviruksen asennus

Ohjelman asennus aloitettiin painamalla ohjelman kuvaketta. Seuraavaksi käyn ohjelman asennusvaiheet vaihe vaiheelta läpi. Tämän jälkeen Windows seiska kysyy, sallitaanko ohjelma suorittaa. Tähän vastataan suorita.

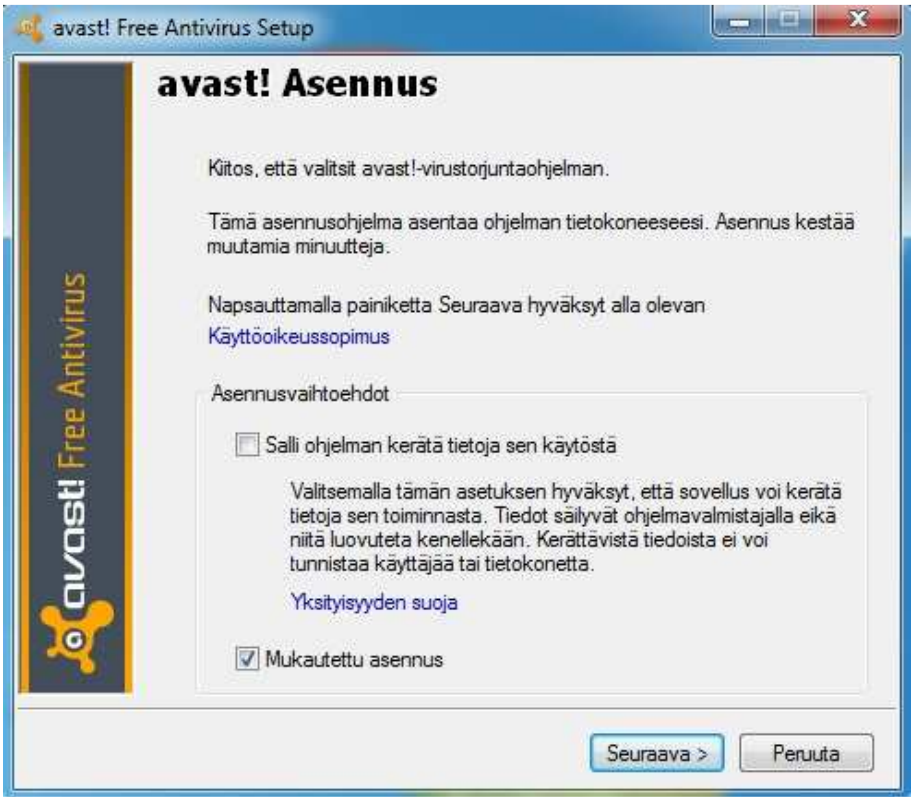


Kuva 1 Windows seiskan varoitus

Seuraavaksi ohjelman asennusikkuna aukesi. Tämän jälkeen valitaan kieli ja painetaan hiirellä seuraava.

Kuva 2 Kielen valinta

Seuraavaksi hyväksytään käyttöoikeussopimus ja valitaan asennusvaihtoehto. Valitsin mukautettu asennus koska en halunnut, että Avast virustorjunnan käyttöä seurataan tietokoneellani.

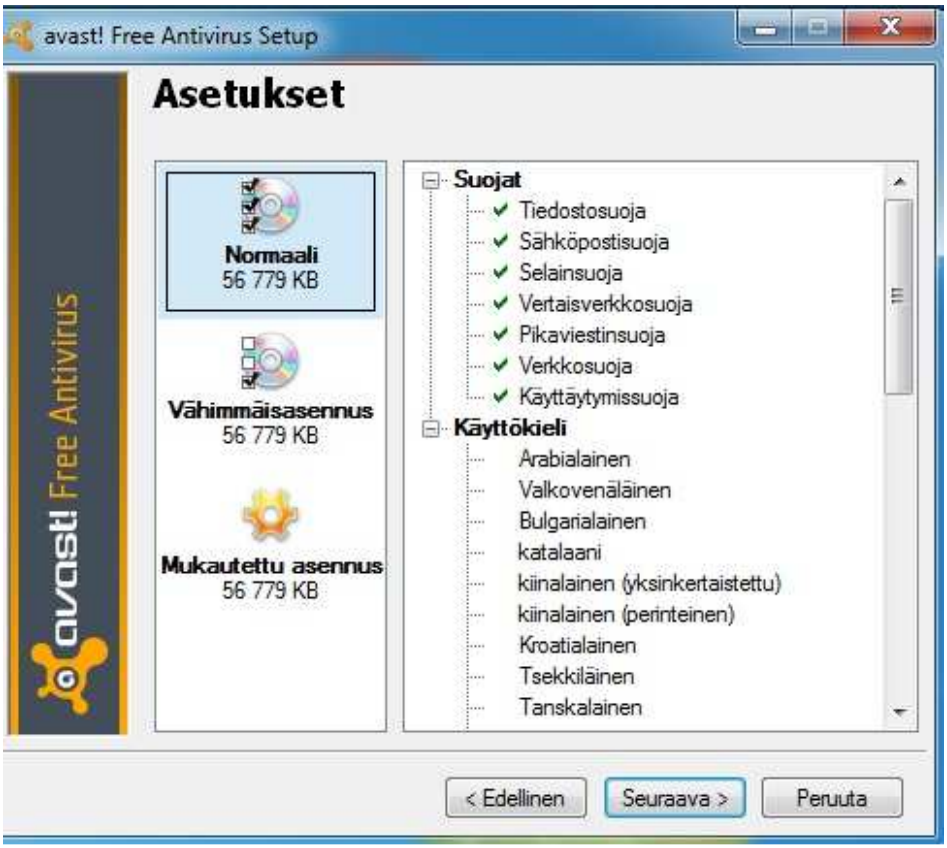


Kuva 3 Asennusvaihtoehto

Tämän jälkeen valitaan kohdekansio, jonne Avast Antivirus ohjelmisto halutaan asentaa.

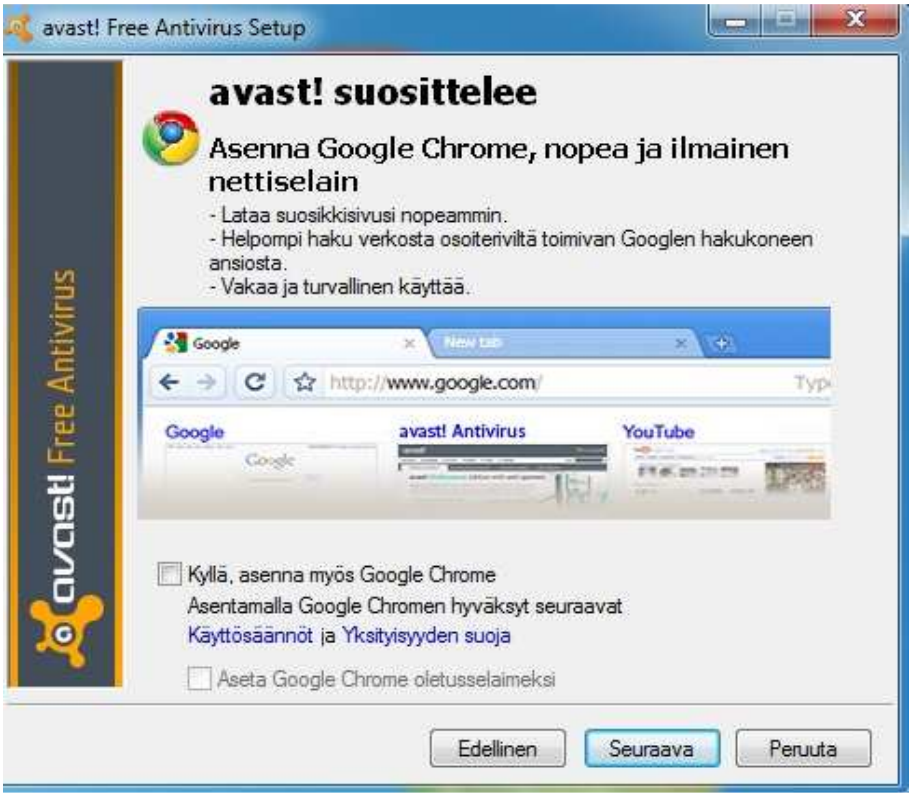
Kuva 4 Kohdekansio

Seuraavaksi valitaan asennuksen tyyppi. Valitsin normaalin asennuksen, koska halusin tutkia Avast Antiviruksen kaikkia hienoja ominaisuuksia.



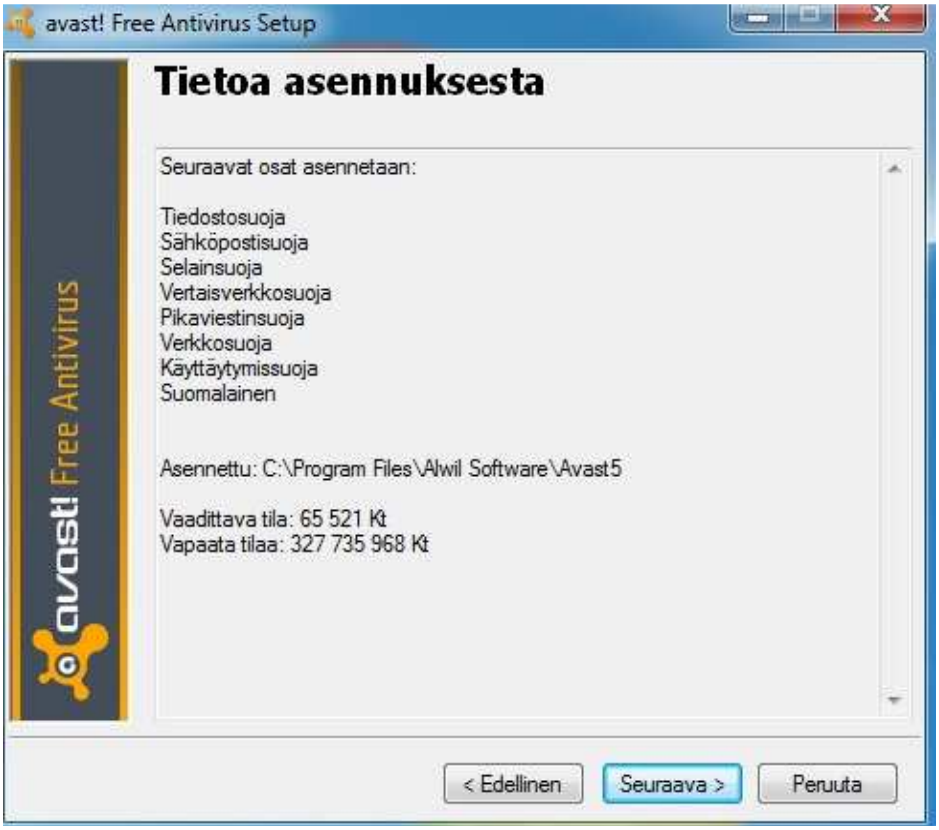
Kuva 5 Asennusvaihtoehdot

Avast Antivirus mahdollistaa Google Chrome -nettiselainasennuksen, mutta sitä ei asenneta.



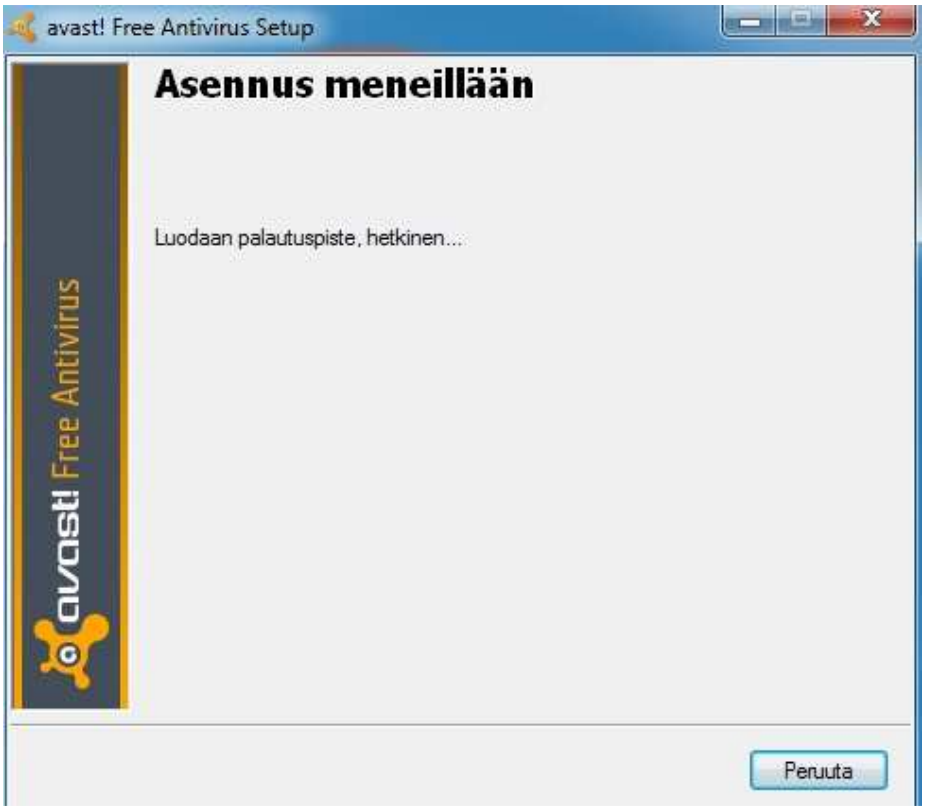
Kuva 6 Google Chrome

Google Chromen asennuksen jälkeen nähdään, mitä ohjelman asennus asentaa ja kuinka paljon asennus vie tilaa.



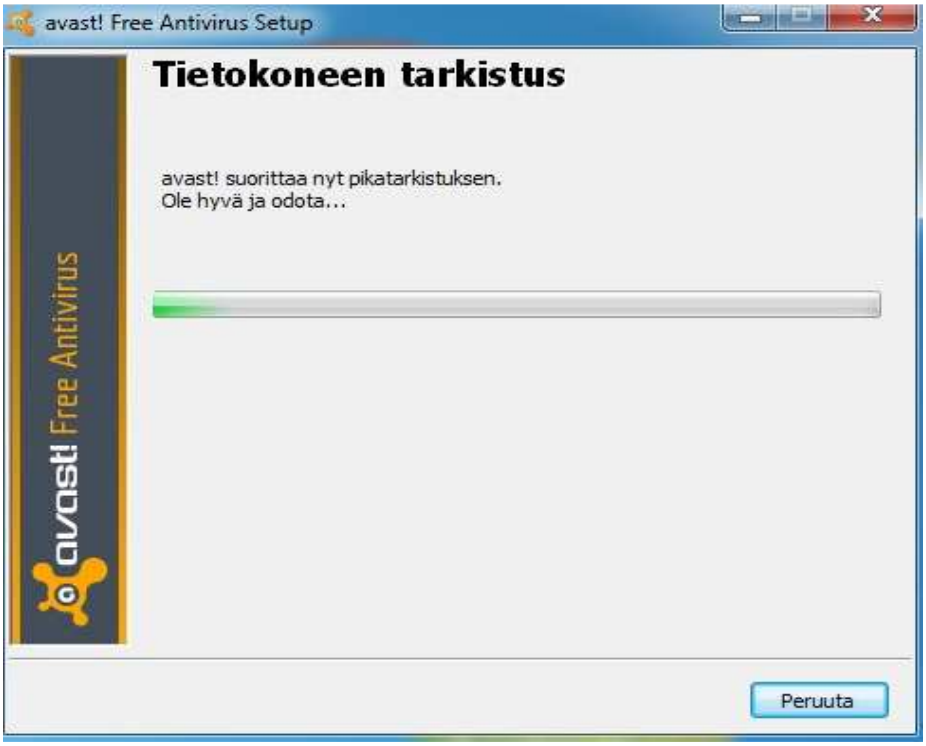
Kuva 7 Asennuksentiedot

Asennustietojen jälkeen Avast Antivirus -asennus luo palautuspisteen Windows seiskalle. Jos asennus sotkee tietokoneen, on tietokone mahdollista palauttaa palautuspisteeseen ja sitten voidaan asentaa Avast uudelleen.



Kuva 8 Palautuspisteen luonti

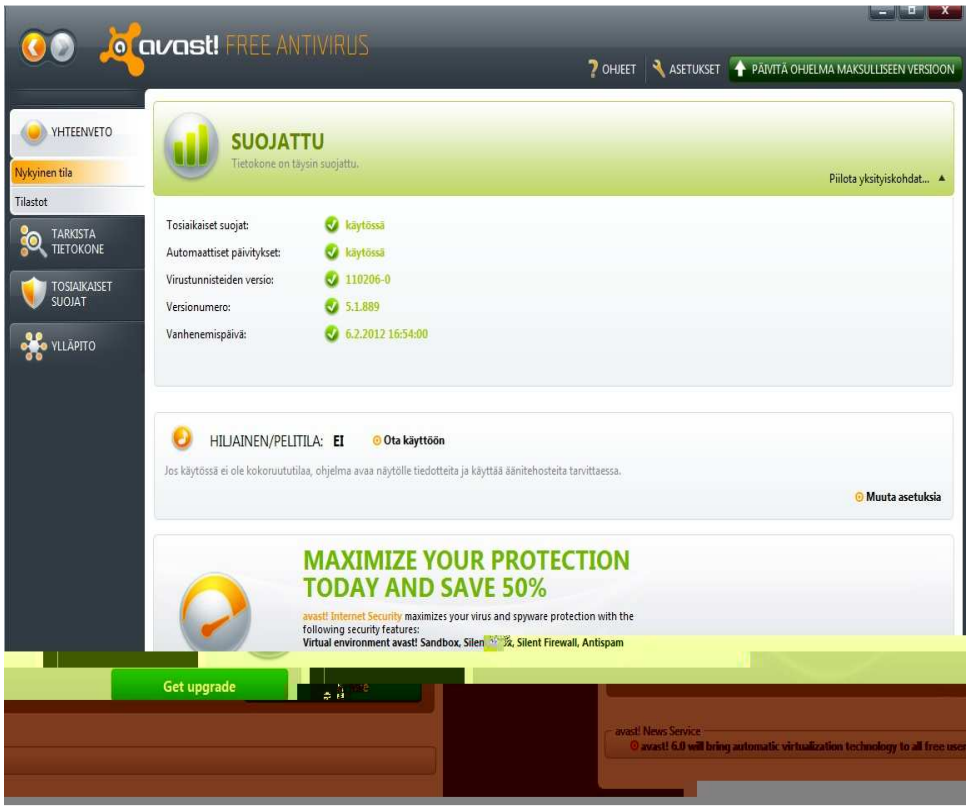
Palautuspisteen luomisen jälkeen tietokone tekee pikatarkistuksen tietokoneelle. Tietokone kannattaa kuitenkin tarkistaa uudelleen, kun Avast Antivirus on päivittänyt virustietokannat. Pikatarkastus ei vienyt kauaa aikaa.



Kuva 9 Pikatarkistus

3.2 Ensimmäinen käynnistys

Ensimmäisen käynnistyksen jälkeen Avast antivirus käynnistyy automaattisesti Windows seiskan käynnistyksessä. Avast päivittää itsenäisesti virustietokannat ensimmäisen käynnistyksen jälkeen. Tämän jälkeen kannattaa tarkistaa tietokone viruksien ja haittaohjelmien varalta Avastilla. Avastin ikkunasta kannattaa tarkistaa, että automaattiset päivitykset, suojaukset ja uusin versio on käytettävissä.



Kuva 10 Avast Antivirus perusnäkymä

3.3 Avast Antiviruksen rekisteröinti

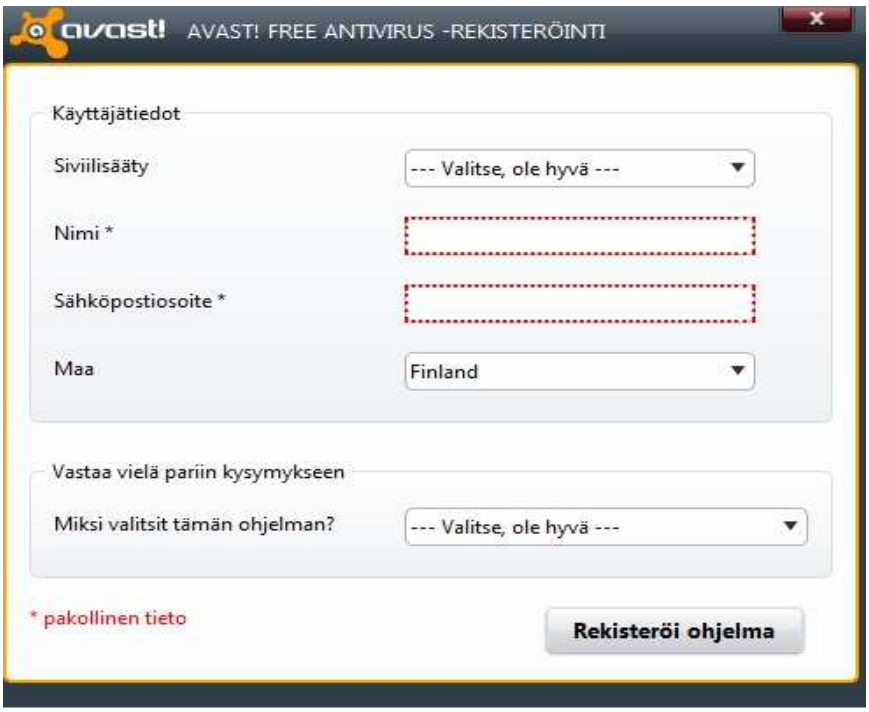
Avast Antivirus ohjelmisto kannattaa rekisteröidä, koska ohjelma ei enää päivitä virustietokantoja 30 päivän jälkeen. Rekisteröinnin jälkeen rekisteröinti on voimassa vuoden, jonka jälkeen se vahvistetaan uudelleen. Rekisteröinti aloitetaan painamalla ”rekisteröi nyt”-nappia.

Kuva 11 Rekisteröinti

Tämän jälkeen ohjelma yrittää tarjota maksullista koko versiota, mutta valitaan rekisteröinti. Avast Antiviruksen koko versiossa on enemmän suojaustiloja, siinä voi muokata paremmin kaikkia asetuksia ja se sisältää myös palomuuri-ohjelmiston.

Kuva 12 Rekisteröinti valinta

Seuraavaksi täytetään käyttäjäkaavake. Tämän jälkeen ohjelma ilmoittaa että rekisteröinti on onnistunut.



Kuva 13 Rekisteröinti

3.4 Valikot ja sisältö

Yhteenveto-valikosta näkee erilaisia tietoja. Yhteenveto-valikko tarjoaa tietoja mm. virusturvan versiosta, päivityksistä ja suojauksen tasosta. Valikko sisältää myös tilastot, joista voi katsoa reaaliaikaisen tarkistuksen diagrammin. Diagrammi sisältää tiedon tarkistetuista tiedostoista.

Tarkista tietokone-valikko sisältää pikatarkistuksen, koko tietokoneen tarkistuksen, siirrettävien muistien tarkistuksen ja valittavat tarkistettavat kohteet.

Pikatarkastus tarkistaa tärkeimmät järjestelmäntiedostot ja keskusmuistin. Koko tietokoneen tarkistus tarkastaa koko tietokoneen ja se vie aikaa huomattavasti enemmän kuin pikatarkastus. Siirrettävien muistien tarkistus tarkistaa kytketyt ulkoiset muistit, esim. muistitikut ja muut siirrettävät muistit. Valittavissa kohteissa voi valita esimerkiksi kansion ja tarkistaa se. Tarkista tietokone-valikko sisältää myös tarkistuksen käynnistyksen alussa -valikon josta voi ottaa sen käyttöön. Tarkistusraportit näyttää kaikki suoritetut tarkistukset tietokoneella.

Tosiaikaiset suojat sisältävät tiedostojärjestelmäsuojan, sähköpostisuojan, pikaviestisuojan, verkkosuojan ja käyttäytymissuojan. Tiedostojärjestelmäsuoja on tärkein suojaus, koska se valvoo kaikkia ohjelmia ja tiedostoja tietokoneella. Diagrammista näkee kuinka paljon tiedostoja tarkastetaan sillä hetkellä. Sähköpostisuoja tarkistaa saapuvat ja lähtevät sähköpostit. Selainsuoja valvoo nettiselaimen ja verkon välistä yhteyttä. Pikaviestisuoja suojaa pikaviestiohjelmista tulevilta viruksilta ja verkkosuoja valvoo verkkoliikennettä. Käyttäytymissuoja tarkkailee tietokoneen toimintaa ja kertoo jos se havaitsee jotakin epäilyttävää.

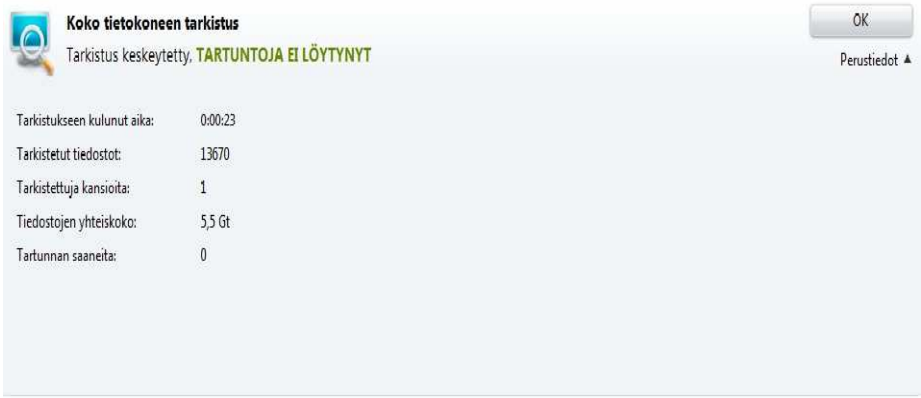
Lisäsuojaus-valikko sisältää lisäsuojauksia. Autosandbox-toiminnon avulla voi suorittaa minkä tahansa epäilyttävän ohjelman hiekkalaatikossa. hiekkalaatikko on muusta tietokoneen tiedostoista eristetty ympäristö. Hiekkalaatikkoon voi lisätä haluamiaan asetuksia, mm. kun tiedosto avataan. Webrep on moduuli jonka avulla Internet-selaimen nettisivuja voi tarkastella maineluokitusten mukaan. Sivujen esto -valikolla voidaan estää pääsy tietyille sivuille

Ylläpito-valikko sisältää tietoja liittyen päivitykseen, rekisteröintiin ja sieltä voi katsoa viruskaranteenissa olevat virukset. Valikosta löytyy myös puitteet, joilla voidaan päivittää ohjelma manuaalisesti.

Valikossa voi muokata ohjelman toimivuutta erilaisin tavoin. Siellä voi valita, miten ohjelma ilmoittaa viruksista ponnahdusikkunalla ja erilaisia äänitehosteita voi säätää. Siellä voi myös muokata viruskaranteenin kokoa ja määrittää salasanan ohjelmalle, ettei kukaan muu voi säätää asetuksia kuin tietokoneen ylläpitäjä.

3.5 Virustarkistus ja muu käyttöopastus

Virustarkistus aloitetaan valitsemalla tarkista tietokone-valikko ja sitten voidaan valita, kuinka tarkasti tietokone tarkistetaan. Tietokone olisi hyvä tarkastaa kokonaan.



Kuva 14 Tietokoneen tarkistus

3.6 Viruksen poisto

Tutkimuksessa simuloitiin tapahtuma, joka voi sattua kenelle tahansa. Tutkimuksessa ladattiin F-Securen sivuilta EICAR-testitiedosto, jonka avulla tutustuttiin virustorjunnan toimintaan tositoimissa. EICAR-testitiedosto on vaaraton tietokoneelle, mutta se toimii viruksen tavoin. Virustorjunta tunnistaa testitiedoston virukseksi. Avast estää Internet-selainta avaamasta/tallentamasta tiedostoa tietokoneelle palvelimelta.

Kuva 15 Haittaohjelma

Toisessa tutkimuksessa luotiin tekstitiedosto, joka sisälsi testikoodia virustorjunnan testausta varten. Tekstitiedoston luomisen jälkeen tutkimuksessa avattiin testitiedosto. Avast tunnisti tiedoston virukseksi ja laittoi sen karanteeniin. Tämän jälkeen virus voidaan poistaa karanteenista. Tiedosto voidaan myös nimetä, jolloin virus ei enää toimi.

4 MICROSOFT SECURITY ESSENTIALS

Microsoft tarjoaa Windowsille omaa virusturvaa, joka on ilmainen. Microsoft Security Essentialsin avulla käyttäjä voi turvata tietokoneensa haittaohjelmia ja viruksia vastaan. Microsoft Security Essentials toimii itsenäisenä sovelluksena taustalla. Ohjelman perusperiaate on sama kuin Avast Antivirus, mutta Avast on kehitetty pidemmälle ja siinä on paremmat tietoturva ominaisuudet muun muassa reaaliaikaiselle tarkistukselle.
(Microsoft Essentials, 2011.)

4.1 Järjestelmä vaatimukset

Microsoft Security Essentialsin järjestelmävaatimukset löytyvät taulukosta 2.

Taulukko 2 Järjestelmävaatimukset

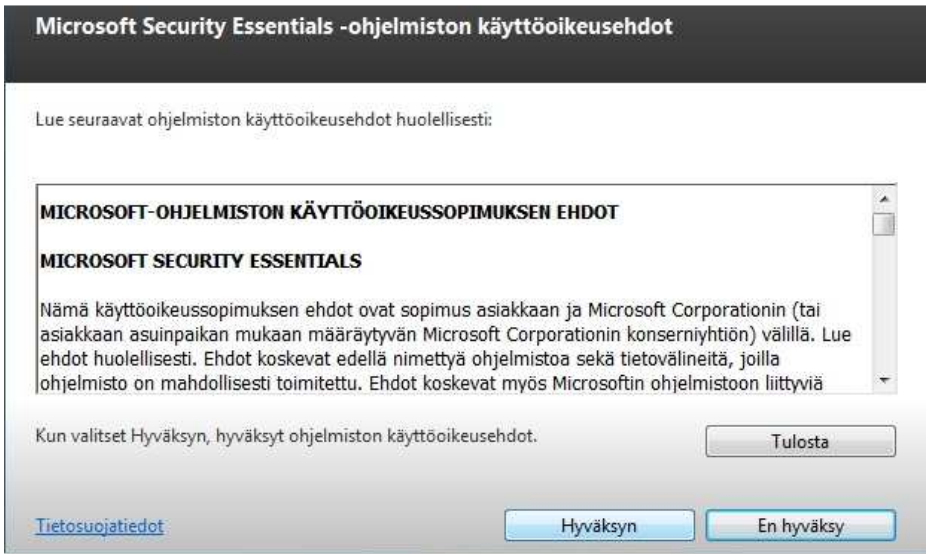
käyttöjärjestelmä	Suoritin	RAM-muisti	näytön tarkkuus	kovalevytila	Internet-selain
Windows XP	650MHz	512 Mt	800 x 600	200 Mt	Firefox tai Explorer
Windows 7	1,6 GHz	1 Gt	800 x 600	200 Mt	saman vaatimukset kuin XP:ssä

4.2 Ohjelman asennus

Microsoft Security Essentialsin asentaminen käy helposti. Seuraavaksi käymme läpi sen asennuksen. Ensimmäiseksi ohjelma ladataan Microsoftin Internet-sivuilta. Tämän jälkeen ohjelma avataan. Seuraavaksi jatketaan valitsemalla seuraava.

Kuva 16 Asennuksen aloitus

Tämän jälkeen Microsoft Security Essentials-ohjelmiston käyttöehdot luetaan tarkasti ja hyväksytään ne.

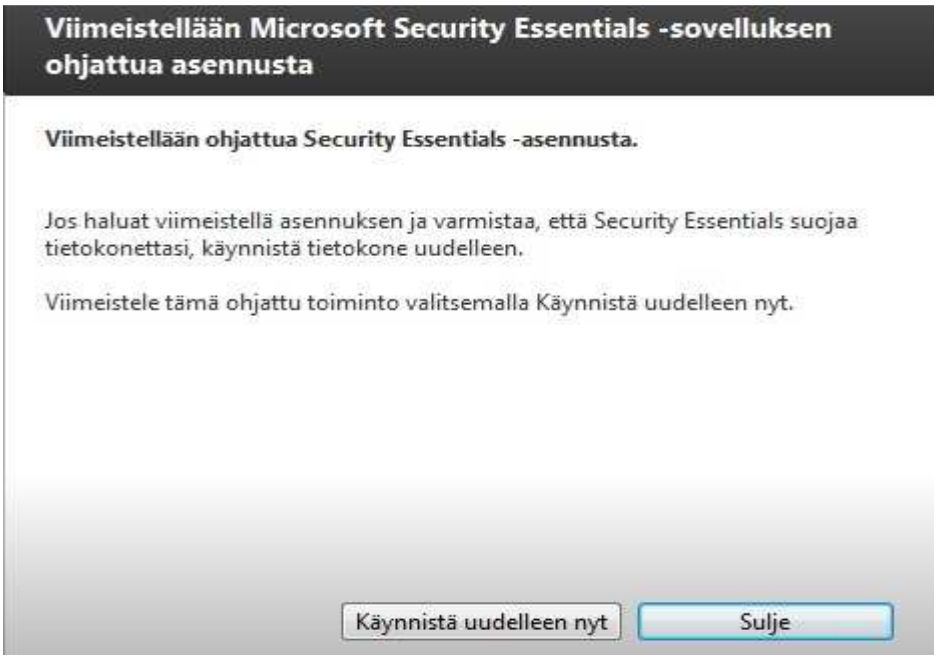


Kuva 17 Käyttöoikeusehdot

Seuraavaksi asennus asentaa ohjelmiston tietokoneella.

Kuva 18 Asennus meneillään

Tietokone kannattaa käynnistää uudelleen ja sen jälkeen kannattaa päivittää virustietokannat ohjelmaan.



Kuva 19 Tietokoneen käynnistäminen uudelleen

4.3 Ohjelman käyttö

Kun tietokone on käynnistetty uudelleen, niin ohjelma on käyttövalmis. Microsoft Security Essentialsin käyttö on helppoa. Etusivulla voi valita, kuinka laajasti tietokone tarkistetaan mahdollisia viruksia vastaan. Päivitä-valikossa voidaan päivittää ohjelma ja historiasta näkee havaitut virukset ja haittaohjelmat tietokoneessa. Asetus-valikossa voidaan ajoittaa tarkistuksia ja määrittää millaiset tiedostot tarkistetaan. Microsoft Security Essentials kerää tietoja ohjelmiston tiedoista ja havainnoista. Ohjelma lähettää tiedot Microsoftille ja uudet tiedot auttavat ohjelmistokehittäjiä ohjelman kehityksessä.

5 PALOMUURIN KÄYTTÖ

Palomuuri voi olla ohjelma tai laite, esimerkiksi reititin, joka tarkistaa verkosta tulevat tiedot. Tulevat tiedot joko estetään tai päästetään tietokoneeseen. Palomuuri päästää tiedot tietokoneeseen, jos ne näkyvät säännöissä. Palomuuri estää luvattomia käyttäjiä ja haittaohjelmia käyttämästä tietokonetta Internetin yli.
(Wikipedia, 2011.)

5.1 Tekniikka

Palomuuri on yksinkertaisuudessaan pakettisuodatin ja se suodattaa paketit osoitteiden ja porttien perusteella. Palomuuri tyyppejä on kahdenlaisia tilallisia ja tilattomia. Tilaton palomuuri käyttää säännöstöä apuna, eli jos paketti ei ole sallittu, sitä ei lähetä eteenpäin. Tilallinen palomuuri on tarkempi valvonnan puitteissa.

Tilallinen palomuuri tallentaa lokitiedostoon TCP ja UDP-yhteyden tiedot ja se sallii niiden yhteyteen liittyvät paketit. TCP -yhteydet tutkitaan ja tarkastetaan että tilasiirtymä on laillinen. Tilattomassa palomuurissa yksi heikko kohta on se, että kaikissa protokollissa ei voida tietää paluupakettien portteja tarpeeksi tarkasti. Tilallinen palomuuri tarkistaa jokaisen paketin ja sen yhteyden. Silloin kun TCP-yhteys avataan, tutkitaan onko yhteys sallittu palomuurin omien sääntöjen mukaan. Uudet hyväksytyt yhteydet lisätään yhteyslistaan. Yhteyksien sulkeutuessa tiedot poistetaan listalta eikä siihen liittyviä paketteja päästetä läpi. Kummassakin on ongelmia tuntemattomien protokollien kanssa mutta niitä voi tarvittaessa lisätä palomuurin listaan. Pakettisuodatin toimii kuljetuskerroksessa.

Hyvänä vaihtoehtona on sovelluspalomuuri. Sovelluspalomuuri tarkistaa paketin sisältämää dataa. Sovelluspalomuuri toimii sovelluskerroksessa. Monet nykyajan palomuurit ovat tilallisen ja sovelluspalomuurista yhdistelmiä. Sovelluspalomuurin etuna on se että sovellus voi päättää sallitaanko yhteys ja tiedetään mitkä palvelut ovat sallittuja ja mitkä eivät ole. Tämän lisäksi tiedetään liikenteen kohteet.
(Wikipedia, 2011.)

5.2 Heikkoudet

Palomuurin tärkein tehtävä on suodattaa sen läpi meneviä yhteyksiä. Kuitenkin verkkoon voi päästä muitakin reittejä pitkin, esimerkiksi langattomien lähiverkkojen avulla tai tunkeutumalla toimitiloihin, missä verkko sijaitsee. Palomuuri ei pysty suodattamaan IPSEC -salattuja yhteyksiä joissa ei näy kohdetietokone tai kohdeportti. Sen takia salattu VPN-liikenne viedään eteisverkolle ja sitten voidaan viedä salaamattomana palomuurin läpi uudestaan.
(Wikipedia, 2011.)

5.3 Windows palomuuri

Windows palomuuri on osa Windows seiska käyttöjärjestelmää. Palomuuri on kehitetty jo vuonna 2001 Windows Xp:lle, tosin silloin palomuuri ei ollut niin monipuolinen kuin Windows seiskassa.

Microsoft alkoi kehittää Windowsin palomuuria sen jälkeen kun useat madot saastuttivat Windows Xp:n käyttöjärjestelmiä ympäri maailmaa. Windows seiskan palomuuria on siis paranneltu huomattavasti. Seiskan palomuuri mahdollistaa etähallinnan ja siinä on Ipv6 yhteyssuodatin. Palomuuriin voidaan myös luoda erilaisia profiileja, esimerkiksi pelimoodi jossa avataan tietty portti juuri sitä peliä varten. Seiskan palomuuri on pakettisuodatin palomuuri jossa voi määritellä sallitut portit ja porttialueet ovat myös mahdollisia. Palomuurissa voi myös sallia erilaisia ohjelmia tiettyihin portteihin.
(Microsoft palomuuri, 2011.)

5.4 Windows-palomuurin ominaisuuksia

Windows seiskan palomuuri mahdollistaa kaiken verkkoliikenteen suodattamisen. Ulospäin menevää liikennettä ei ole kauhean helppo rajoittaa, koska palomuuri ei osaa avata ikkunaa jossa voitaisiin sallia tai hylätä ohjelman pääsy ulkoverkkoon. Palomuurin säännöt on luotava palomuurin hallinnassa. Palomuurissa voi määritellä suojaustasoja esimerkiksi kotiin koti- ja työhön työsuojaustalo. Suojausprofiileja on helppo vaihtaa puolin ja toisin.

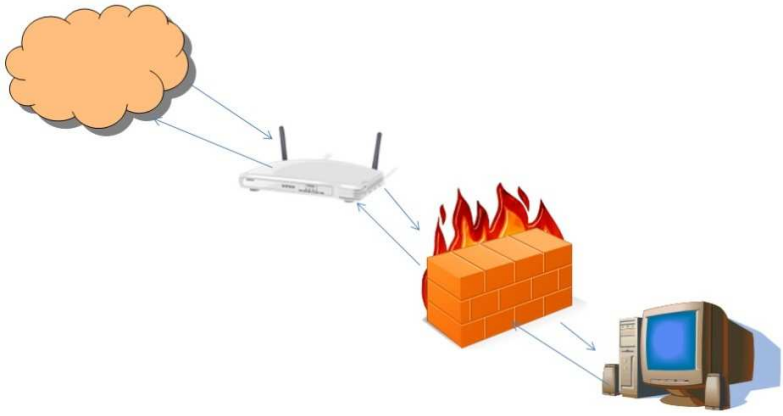
5.5 Järjestelmänvaatimukset ja testausympäristö

Windows seiskan palomuurin järjestelmävaatimukset eivät vaadi paljoa, riittää että Windows seiska toimii. Testausympäristö rakentuu itse kootulle tietokoneelle. Koneen kokoonpano selviää taulukosta 3.

Taulukko 3 Testitietokone

Prosessori	Intel DualCore 3,7 Ghz
emolevy	Msi
keskusmuisti	2 Gt DDr2
verkkokortti	1000 Mbit
cd-asema	on
Käyttöjärjestelmä	Windows 7

Valitsin Windows seiskan tietokoneelle, koska monet kotikäyttäjät käyttävät tai ovat suunnittelemassa Windows seiskan käyttöä kotona. Internetyhteytenä toimii 10Mbit/1Mbit Internet-liittymä. Kuvassa 20 näkyy verkkotopologia testiympäristössä.



Kuva 20 Verkkotopologia

5.6 Palomuurin testaus Shield Up -sivusto

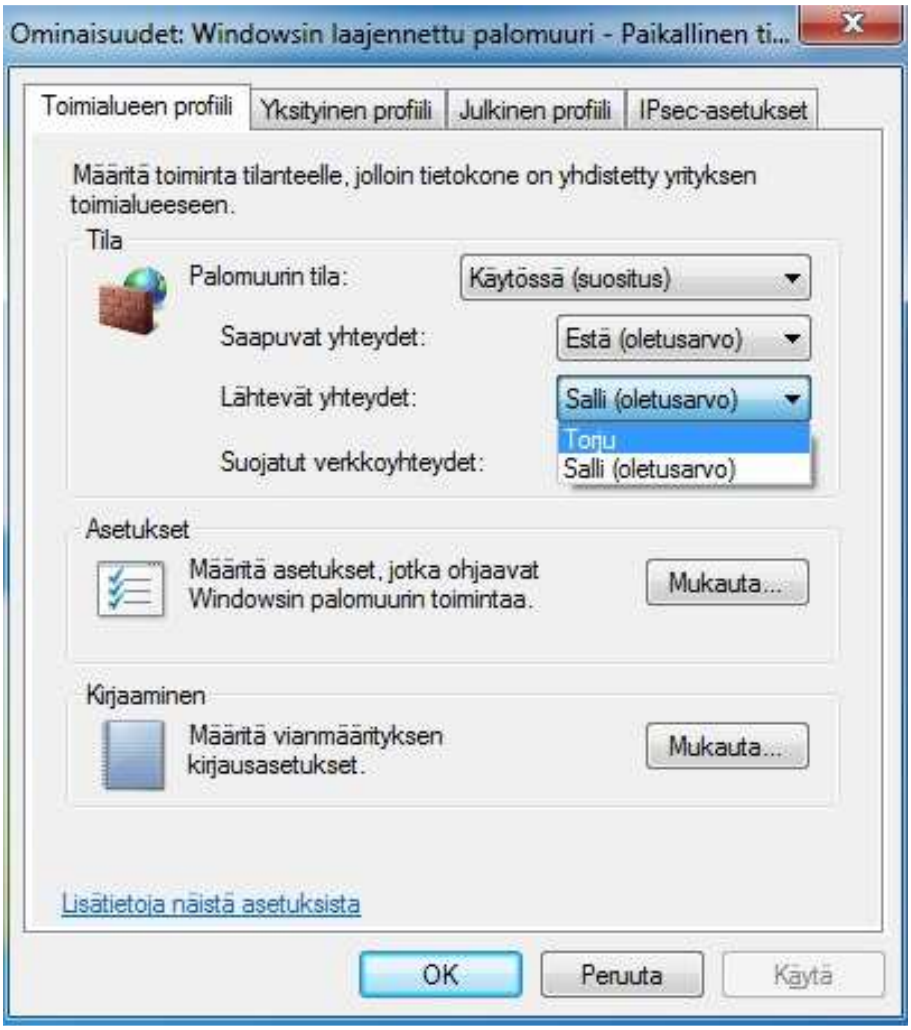
Shield Up -sivustolla voi testata palomuurin toimivuutta. Sivusto tarjoaa laajat mahdollisuudet testata palomuurin sääntöjä mm. portteja ja testata Windowsin palveluita tietoturvan kannalta.
Seuraavaksi testaamme palomuurin toimivuutta erilaisilla testeillä jotka sijaitsevat Shield Up -sivustolla.

Port	Service	Status	Security Implications
0	<nil>	Closed	Your computer has responded that this port exists but is currently closed to connections.
21	FTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
22	SSH	Closed	Your computer has responded that this port exists but is currently closed to connections.
23	Telnet	Closed	Your computer has responded that this port exists but is currently closed to connections.
25	SMTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
80	HTTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
110	POP3	Closed	Your computer has responded that this port exists but is currently closed to connections.
113	IDENT	Closed	Your computer has responded that this port exists but is currently closed to connections.
119	NNTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
135	RPC	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
139	Net BIOS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

Kuva 21 Shield Up yleiset portit

Common Port-testillä voidaan tarkistaa, että yleisimmät portit ovat kiinni. Yllä olevassa kuvassa näkyy että portit on kiinni. All ports -testillä voidaan katsoa aivan kaikki portit.

Palomuuri on valmiina Windows seiskan käyttöjärjestelmässä. Seuraavaksi asetamme palomuurin suodattamaan myös lähteviä yhteyksiä, joita ei ole estetty oletuksena. Ensimmäiseksi avataan palomuurin toiminnot -valikosta välilehti ominaisuudet. Sitten kaikissa profiileissa tehdään seuraava toimenpide, eli torjutaan lähtevät yhteydet kaikissa profiileissa.
(Muurinet, 2010.)



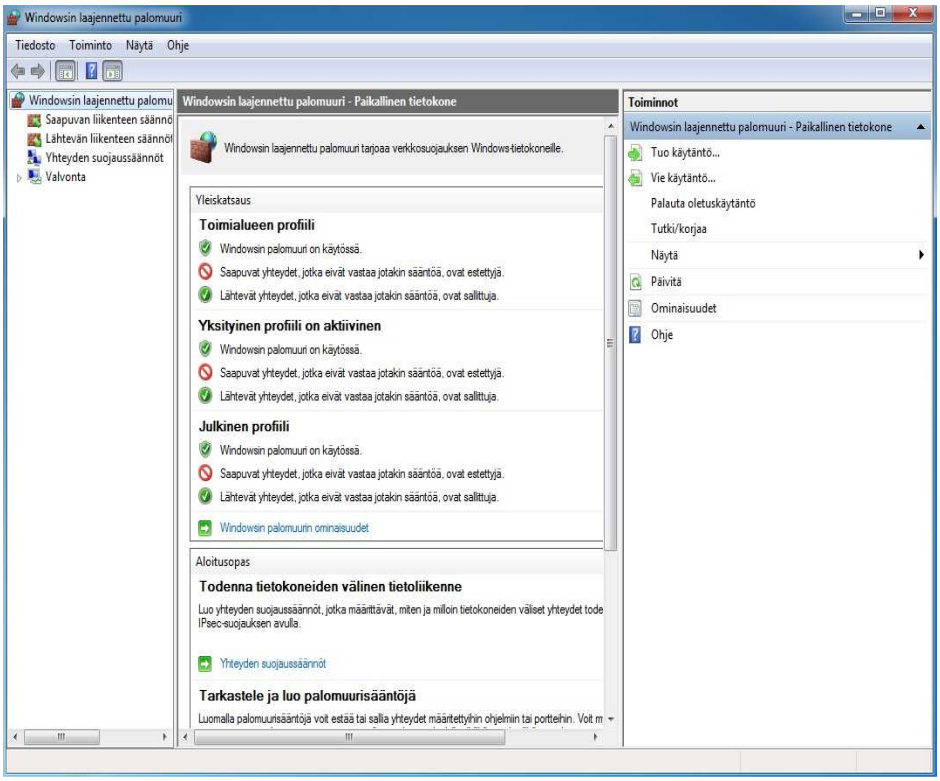
Kuva 22 Lähtevät yhteydet

Tämän jälkeen Internet-selaimelle tehdään säännöt, jotta tietokoneella pääsee Internetiin. Seuraavaksi klikataan lähtevän liikenteen sääntöihin ja lisätään uusi sääntö. Tämän jälkeen valitaan ohjelma-valikko ja etsitään ohjelma ohjelmapolun avulla. Tämän jälkeen sallitaan Internet-selain kaikilla profiileilla.
(Muurinet, 2010.)

Aloittelijoiden on mahdollista päästä helpommalla asentamalla Windows seiskan firewall control -ohjelman. Suosittelen tätä ohjelmaa, koska sillä voi luoda helposti ja nopeasti palomuurisääntöjä ilman ongelmia. Ohjelma käyttää Windows palomuuria, eikä se asenna mitään ylimääräisiä laajennuksia Windows seiskaan. Ohjelmisto toimii niin, että se ilmoittaa kun jokin tietokoneella oleva ohjelma haluaa ottaa yhteyden Internetiin. Ilmaisversiossa kaikki lähtevät yhteydet torjutaan ja maksullisessa versiossa sääntöjä voidaan muokata tarkemmin jokaiselle ohjelmalle erikseen.

5.8 Palomuurin käyttö

Windows seiskan palomuuri on päällä automaattisesti. Windows seiskan palomuuri löytyy ohjauspaneelista. Windows seiskan palomuurin laajennettu versio löytyy Windows-palomuurin ikkunasta ja siellä olevasta lisäasetuksista.



Kuva 23 Windows seiskan laajennettu palomuuri

5.9 Valikot

Yleisvalikosta nähdään erilaisia tietoja palomuurista ja sen asetuksista. Saapuvat liikenteen ”säännöt” -valikossa näkee saapuvan liikenteen sääntöjä joita voi muokata ja suodattaa. Lähtevä liikenne- säännöt löytyvät saapuvan liikenteen alapuolelta. Lähtevän liikenteen -säännöt poikkeavat siinä

mielessä että suurin osa liikenteestä sallitaan. Yhteyden suojaussäännöissä voidaan luoda eri yhteyksille erilaisia sääntöjä sekä tuleville että lähteville säännöille.

Valvonta-valikosta löytyy tietoja palomuurin senhetkisistä yhteyksistä Internetiin ja erilaisia tiloja joilla voi tehdä omia suojaprofiileja.

5.10 Logit

Windows seiskan palomuuri tallentaa tietoja palomuurin toiminnasta lokiin. Logi kertoo onko yhteyksiä estetty tiettyihin IP-osoitteisiin. Windows tallentaa login järjestelmäntiedostoihin. Lokille voi määrittää enimmäiskoon ja määrittää lähtevien ja tulevien yhteyksien tietoja.

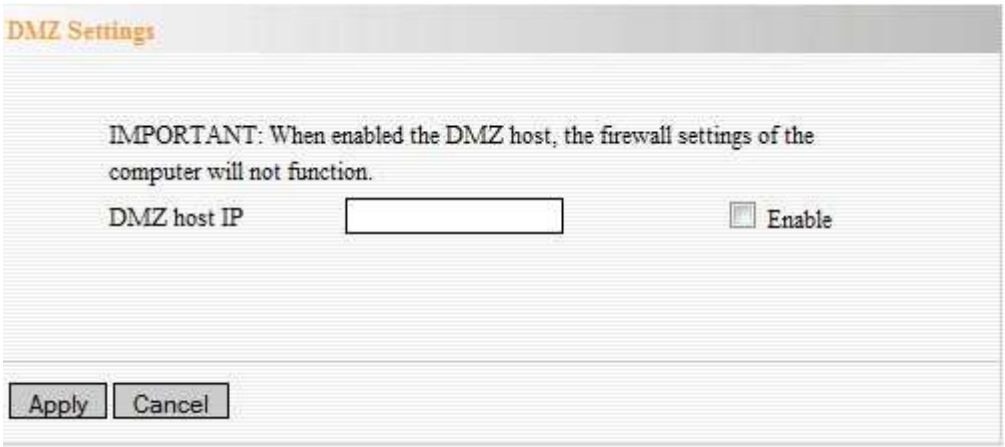
6 NETWJORK TUKIASEMA

Monissa kotitalouksien tukiasemissa ja reitittimissä on erilaisia tietoturvaratkaisuja. Nämä tietoturvaratkaisut eivät kuitenkaan ole riittävät kotiverkon tietoturvaa silmällä pitäen. Seuraavaksi tarkastellaan Netwjork tukiaseman tietoturvaratkaisuja.

Reitittimen UPnP protokollat kannattaa sulkea verkosta, koska sen kautta hyökkääjä voi saastuttaa reitittimen. Reititin voi saastumisen jälkeen hyökätä kotiverkon koneita vastaan. UPnP on oletuksena päällä, mutta se otetaan pois ja painetaan Apply.

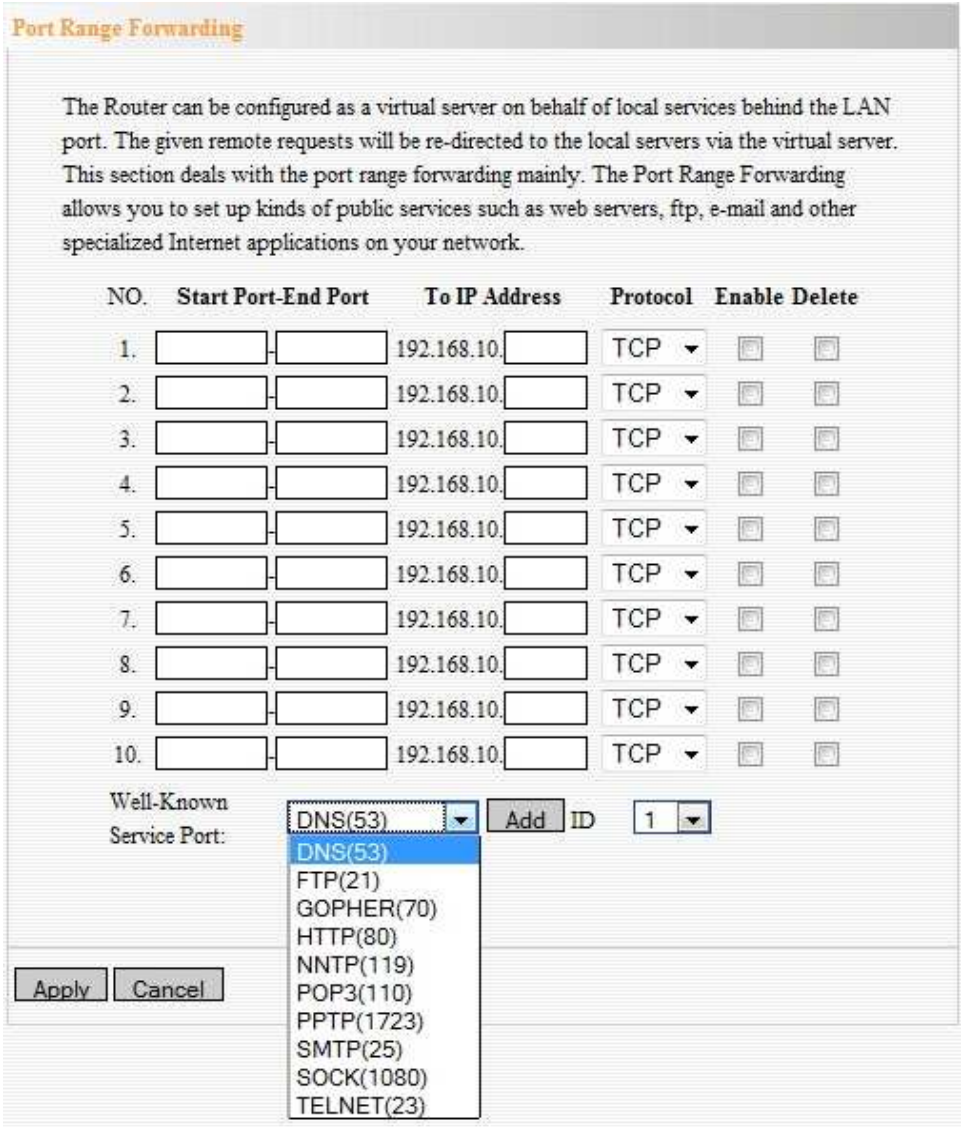
Kuva 24 UPnP Settings

Reitittimen DMZ -alue kannattaa laittaa sellaiseen tietokoneeseen, johon haluaa laittaa verkkopalvelimen. Muuten DMZ -alue kannattaa pitää kiinni. Toisaalta tällöin kotiverkon tietokoneet eivät voi keskustella toistensa kanssa. DMZ -alue määritetään yhdelle koneelle laittamalla sen IP-osoite ja laittamalla enable ja apply.



Kuva 25 DMZ -alue

Porttiohjauksen avulla tietokoneeseen voidaan avata portteja jotta sovellukset saavat yhteyden kotiverkkoon Internetistä. Porttiohjausta ei kannata käyttää turhaan, koska sen avulla hyökkääjä voi hyökätä tietokoneelle avatun portin kautta. Porttiohjaus määritellään lähtö- ja loppu portti sen jälkeen annetaan IP-osoite ja protokolla ja apply.



Kuva 26 Porttiohjaus

6.1 Langattoman verkon suojaus

Langattoman verkon tietoturvasta kannattaa huolehtia. Langattomassa verkossa tieto liikkuu ilmassa eivätkä seinät vaimenna sitä. Tämä tarjoaa ulkopuoliselle hyökkääjälle mahdollisuuden kuunnella langatonta verkkoa jos tietoturvasta ei huolehdita. Hyökkääjä voi tarkastella lähiverkkoa ja tutkia missä Internet-sivuilla on vierailtu.

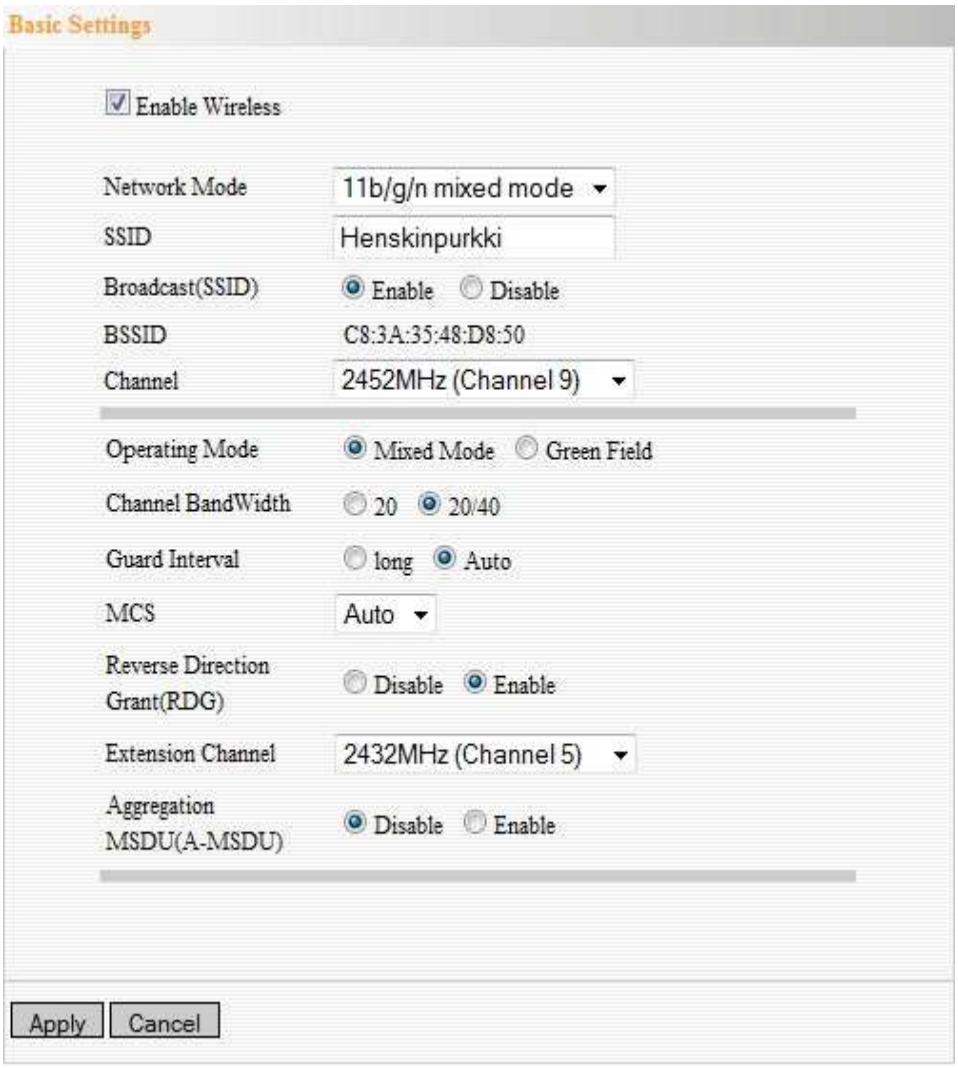
Langattomissa verkoissa on monia erilaisia suojausmenetelmiä, seuraavaksi tarkastellaan tärkeimpiä suojausmenetelmiä. Tärkeimpiä salausmenetelmiä ovat WEP ja WPA -salaus. Kaikki verkkokortit tukevat 64- tai 128-bittistä web-salausta. WEP -salaus on vanhimpia salauksia ja se on suhteellisen helposti murrettavissa kuuntelemalla vaikka aircrack-ohjelmalla verkkoa. Näiden lisäksi kannattaa laittaa Mac-suodatus ja piilotettu SSID päälle. WEP ja WPA tarjoavat riittävän suojan kotikäyttäjille. WPA-salaus on kehitetty WEP -salauksen pohjalta. Yleensä WPA-salaus käyttää WPA-PSK TKIP tyyppiä, jossa on vaihtuva salausavain. WPA-PSK salauksella määritellään jokaiselle tietokoneelle oma salausavain. Tukiasema käyttää salausavainta tietokoneen tunnistamiseen. WPA-PSK riittää hyvin kotikäyttöön. WPAssa verkon tieto suojataan automaattisesti vaihtuvilla salausavaimilla. WPA:sta on olemassa vielä kehittyneempi versio WPA2. WPA 2 -PSK tarjoaa kotikäyttäjälle paremman tietoturvan kehittyneemmillä salausalgoritmilla. WPA 2 -salausta on lähes mahdotonta murtaa nykyisillä tietokoneilla.

Langattomassa verkossa ei siis kannata käyttää WEP-salausta jos kaikkien tietokoneiden Wlan-kortit tukevat kehittyneempää salausta.

Langattoman tukiasemalle on myös muita hyviä suojausmenetelmiä. Tukiaseman signaalia kannattaa pienentää, jolloin verkon kantama pienenee. (Mvnet, 2011.)

6.2 Netwjork langattoman verkon tietoturva

Kun tukiasema oli asennettu valmiiksi, niin seuraavaksi oli määritettävä langattoman verkon tietoturva-asetukset kuntoon. Ensimmäiseksi tukiasemalle annettiin nimi. Tämän jälkeen laitettiin nimen mainostus päälle, koska kaikki verkkokortit eivät saaneet yhteyttä langattomaan verkkoon.

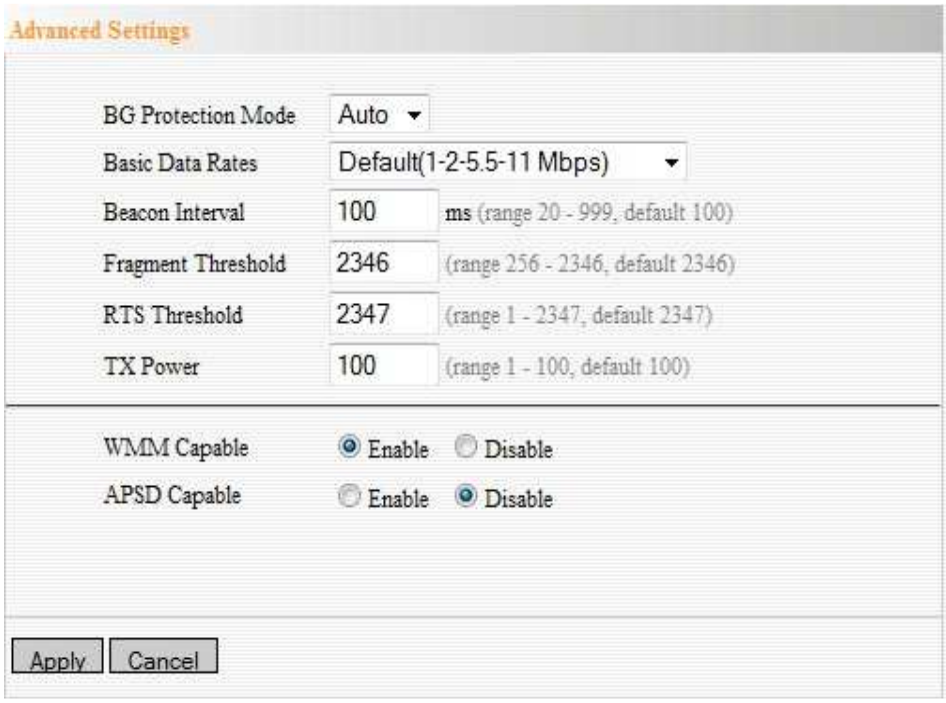


Kuva 27 Perusasetukset

Seuraavaksi määritettiin verkon tietoturvasuojaustaso. Tietoturvatasoksi valittiin WPA 2 -Personal, koska se tarjoaa tarpeeksi vahvan suojan tukiasemalle. WPA kakkoselle valittiin TKIP ja sitten määritettiin tukiaseman perusavain langattomalle verkolle.

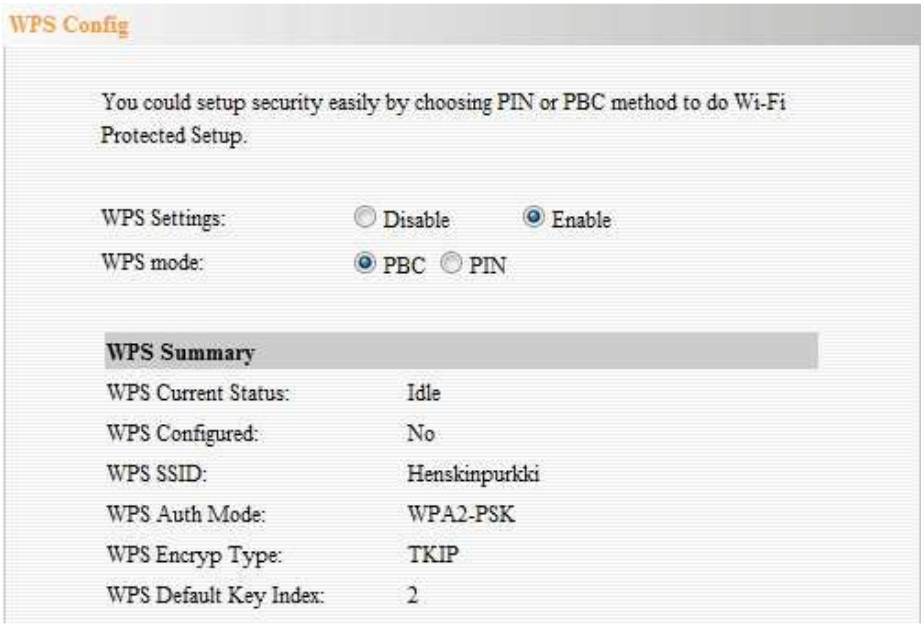
Kuva 28 Verkon määritykset

Perusasetusten jälkeen määritettiin signaalin teho pienemmäksi, jotta verkko ei ulottuisi liian laajalle alueelle kodin ulkopuolelle.



Kuva 29 Lisäasetukset

Seuraavaksi voitiin määrittää tukiasemalle tietoturva-asetukset.



Kuva 30 Tietoturva toiselle tukiasemalle

Tämän jälkeen määritettiin tukiasema torjumaan hyökkäyksiä ulkopuolelta esimerkiksi Smurf attackia vastaan. Tukiasemalta poistettiin etäyhteyden mahdollisuus, koska hyökkääjä voi saada tukiaseman sen portin kautta haltuun.

7 YHTEENVETO

Opinnäytetyön tarkoituksena oli opastaa kotikäyttäjää toimimaan turvallisesti kotiverkossa. Avast Antivirus tarjoaa hyvät mahdollisuudet virusten ja muiden haittaohjelmien torjuntaan. Avast Antivirus toimii myös vanhemmissa koneissa, joissa tietokoneen suorituskyky ei ole enää ajan tasalla. Avast Antivirusta testattiin viruksilla ja Avast torjui ne.

Microsoft Essentials tarjoaa kotiverkon käyttäjälle hyvän virustorjunnan. Opinnäytetyössä testattiin kumpaakin virustorjunta-ohjelmaa. Avast Antivirus ohjelma on parempi, koska se tarjoaa mahdollisuuden muokata laajemmin virustorjuntaa ja se torjuu paremmin virukset ja haittaohjelmat kuin Microsoft Essentials.

Windows seiska palomuuri tarjoaa hyvän perusturvan kotiverkon tietokoneille. Palomuuri on kevyt ja sitä on helppo hallita. Palomuurin ei torju lähteviä yhteyksiä. Kotikäyttäjä voi säätää palomuurin torjumaan lähteviä yhteyksiä tai käyttäjä voi hankkia firewall control -ohjelman jolla on helpompi hallita Windows seiskan palomuuria. Windows seiskan palomuuri testattiin Shield Up -sivuston hyökkäystyökaluilla. Windows seiskan palomuuri toimi hyvin ja palomuurissa oli turhat portit suljettu.

Opinnäytetyössä tarkasteltiin Netwjork reititintä ja sen tietoturvaominaisuuksia. Netwjork reititin tarjoaa paljon mahdollisuuksia hyökkääjiä vastaan. Reititin sisältää sisäisen palomuurin. Palomuurissa on tärkeitä ominaisuuksia ja niitä voi säädellä tarkoitusten mukaan. Netwjork-reitittimen langattoman verkon tietoturva-asetukset oli helppo määrittää. Netwjork tarjoaa hyvät tietoturva ominaisuudet langattoman verkon salaukseen.

WPA 2 salaus tarjoaa hyvän salauksen tukiasemassa, jolloin tukiaseman murtaminen on lähes mahdotonta. Reitittimen etäyhteys kannattaa laittaa pois päältä mahdollisten hyökkääjien varalle. Reititintä testattiin Shield Up -sivuston avulla. Rautapalomuurit eivät ole niin turvallisia kuin ohjelmistopohjaiset palomuurit, joten kotikäyttäjän kannattaa asentaa kaikille tietokoneille ohjelmistopohjainen palomuuri rautapohjaisen palomuurin vierelle. Mac-suodatus kannattaa laittaa päälle, mutta se vain hidastaa hyökkääjää. SSID kannattaa piilottaa mutta se vain hidastaa hyökkääjää.

Avast Antivirus ja Windows seiskan palomuuri riittävät aivan hyvin perustietoturvaan.

LÄHTEET

Avast!, Wikipedia vapaa sanakirja, 2011, Viitattu 23.2.2011,
http://fi.wikipedia.org/wiki/Avast!

Microsoft Essentials, 2011, Viitattu 11.3.2011,
http://www.microsoft.com/security_essentials/default.aspx?mkt=fi-fi

Wikipedia,2011, Palomuuri, Viitattu 11.3.2011,
http://fi.wikipedia.org/wiki/Palomuuri

Microsoft windows palomuuri, 2011, Viitattu 10.2.2011,
http://windows.microsoft.com/fi-FI/windows7/What-is-a-firewall

Mvnet, 2011, Viitattu 1.3.2011,
http://www.mvnet.fi/index.php?osio=Tietokoneet&sivu=Langaton_kotiverkko

Muurinet, Windows 7 / Vista palomuurin asentaminen, 2010, Viitattu 12.2.2011,
http://www.muuri.net/tietoturva/windows-7-vista-palomuurin-asentaminen/

Viestintävirasto Ficora, 2007, Viitattu 10.1.2011,
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/palomuuri.html